UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,907	01/19/2001	Stephen M. Trimberger	X-714 US	9367

24309 7590 02/10/2005

XILINX, INC
ATTN: LEGAL DEPARTMENT
2100 LOGIC DR
SAN JOSE, CA 95124

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 02/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/765,907	TRIMBERGER, STEPHEN M.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/28/2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 9/7/2004, applicant amends claim 9 to correct a minor error. The following claims 1-43 are presented for examination.

2. Applicant's remarks, page 11, filed on 9/7/2004, with respect to the objection of claims 33-43 have been fully considered. The objection has been withdrawn.

2.1 Applicant's arguments, pages 11-18, filed on 9/7/2004, with respect to the rejection of claims 1-43 have been fully considered, but they are not persuasive. Regarding claims 1, 12, 23, and 33, Applicant argues Kean does not teach using a manufacturing process characteristic that is unique to the FPGA relying on an approach (paragraph 0134), which is not cited in the Office Action instead of using the alternative approach (paragraphs 136-141) cited in the Office Action. Examiner respectfully disagrees. Kean teaches "ways to encode key data by setting initial state of a random selection of memory cells (using changes to the masks) out of the hundred of thousands ...) (end of paragraph 0136 to paragraph 0137) that meets the recitation of generating the fingerprint using a manufacturing process characteristic that is unique to the FPGA . Another example for encoding a particular key *(generating fingerprint)* by changing one or more of the optical masks used in manufacturing the chip (hiding less than 200 bits of secure information in the massively complex manufacturing data for the FPGA) also shows a characteristic unique to each FPGA that is manufactured. In addition, paragraph 0104 describes another manufacturing

process in another embodiment that shows uniqueness for example "a mask out of 15 to implement the fingerprint since a mask may have more than 10 million shapes" that meets the recitation of using a manufacturing process characteristic that is unique to the FPGA. (See also paragraphs 0106-0109 for more description of the manufacturing process in generating the fingerprint. Kean discloses the limitations of claim 1 as claimed. Regarding claims 3, 14-16, 25-26, and 35, Applicant argues that Kean does not transmit the key from the FPGA to an encryption circuit. Examiner respectfully disagrees. In paragraph 0055, Examiner asserts that Kean discloses transmitting a fingerprint from a random number generator of the FPGA (meets the recitation of the source of the key being the FPGA) and the key is transmitted to the encryption circuit coupled to the random number generator. Therefore, claims 3, 14-16, 25-26, and 35 are rejected as claimed by Applicant.

Regarding claims 5 and 37, Pearson discloses measuring propagation delays to generate the fingerprint (column 7, line 33 through column 9, line 25). Applicant argues about the suggestion to combine in the rejection of the dependent claims. For instance, Pearson mentions several benefits associated with securing a fingerprint in columns 2-3, such as more sophisticated time-out and randomization and time-dependent electronic keys (column 2, lines 49 through column 3, line 12). As for the citations in US patent to Pearson from the previous Office Action, Examiner provides more direct citations below to make the rejection clearer as requested by Applicant. Also, more prior arts are provided to show evidence of prior art of the techniques used to generate fingerprint (RFC 1750, December 1994) recommends use of truly random hardware techniques for generating fingerprint.

Regarding the other dependent claims, in response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, "the use of truly random hardware techniques is recommended for security" (RFC 1750), and Merritt offers an efficient method using an electronic test key that varies pulse widths and/or periods, and frequencies of other control signals (column 7, lines 7-20) to stress, for instance, the memory device, it prevents failure on a simple test and it provides good production feedback as to where the lockout delays should be adjusted (column 6, lines 4-67). (See also Kean, page 4, paragraph 0053 for suggestion to combine).

Regarding claims 10, 11, 18, 29, and 42-43, Applicant argues that the claimed fingerprint as disclosed is not used to program the FPGA as disclosed in Rodgers. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Rodgers discloses a method that offers several benefits, for example, it makes an interconnection or logic cells predictable, for example implementing embedded macrofunctions and allows the logic so implemented to be available immediately

upon power-up (column 8, lines 28-36). In addition it eliminates timing mismatches (column 8, lines 19-27).

Upon further consideration, for at least the reasons cited above, Applicant has not overcome the prior arts. Therefore, claims 1-4, 12-16, 23-26, and 33-36 remain rejected under 35 USC 102 and claims 5-11, 17-22, and 27-32, and 37-43 are still rejected under 35 USC 103.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3.1 **Claims 1-4, 12-16, 23-26, and 33-36** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Publication US 2001/0037458 to **Kean**.

3.2 **As per claims 1, 12, 23, and 33, Kean** discloses a method a FPGA and apparatus of securing communication of configuration data between a field programmable gate array (FPGA) and an external storage device comprising: a plurality of configurable logic elements within the FPGA being programmable with configuration data to implement a desired circuit design, for example (see page 10, paragraphs 0136-0141); generating a fingerprint within the FPGA, the fingerprint representing an inherent manufacturing process characteristic unique to the FPGA, for example (see page 10, paragraphs 0101-0109; 0136-0141); a storage device external to the FPGA, the storage device for storing encrypted configuration data and transmitting encrypted configuration data from the storage device to the FPGA, for example (see page 5, paragraphs 0055 and page 4, paragraph 0041); and decrypting the encrypted configuration data in the FPGA using the fingerprint as a decryption key to extract the configuration data, for example (see page 4, paragraph 0041).

As per claims 2, 13, 24, and 34, Kean discloses the limitation of further configuring the FPGA using configuration data, for example (see page 10, paragraphs 0136-0141 and page 6, paragraph 0067).

As per claims 3, 14-16, 25-26, and 35, Kean discloses the limitation of further comprising: transmitting the fingerprint from the FPGA to an encryption circuit, for example (see page 5, paragraph 0055); encrypting the configuration data using the fingerprint as an encryption key, for example (see page 5, paragraph 0055); and storing the encrypted

configuration data in the storage device, for example (see page 5, paragraphs 0055 and see page 1, paragraph 0009).

As per claims 4 and 36, Kean discloses the limitation of, wherein the fingerprint generated during power-up of the FPGA, for example (see page 10, paragraph 0136).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 5, 9, 17, 19, 27, 28, 37 and 41** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2001/0037458 to **Kean** in view of US Patent 5,838,256 to **Pearson et al.**.

4.2 **As per claims 5, 19, 27, and 37, Kean** substantially teaches the claimed method and apparatus of claims 1, 12, 23, and 33. **Kean** also discloses generating fingerprint from a

plurality of circuit elements, for example (see page 10, paragraphs 0134-0141). **Kean** also suggests create wires which attach to the key input in complicated pattern into the surrounding circuit and changing conductive layer and direction at regular intervals to make it difficult for an attacker to trace them. **Kean** further discloses by using masking technique the need for on-chip volatile memory is removed. **Kean** does not explicitly disclose using propagation delays. This technique is well known in the art to generate fingerprint. However, **Pearson et al.** in an analogous art teaches a method of measuring propagation delays and combining the propagation delays to generate signals to provide security to prevent attacker to crack the electronic key, for example see (column 7, line 33 through column 9, line 25). Pearson mentions several benefits associated with securing a fingerprint in columns 2-3, such as more randomization and time-dependent electronic keys. Therefore, it would have been obvious to one of ordinary skill in the art of integrated circuit at the time the invention was made to modify the method of **Kean** to measure propagation delays for a plurality of circuit elements on the FPGA and combine the propagation delays to generate the fingerprint as taught by **Pearson et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Pearson et al.** so as to provide an electronic key hardware module which is harder to crack, time-dependent operations, and more sophisticated random output function (columns 2-3).

As per claims 9, 17, 28, and 41, Kean substantially discloses the claimed method and apparatus of claims 1, 12, 23, and 33. **Pearson et al.** discloses the limitation of providing a plurality of line segments on the FPGA, determining whether a width of each line segment is less

than a predetermined value, and means for generating, for each line segment, a corresponding bit of the fingerprint in response to the determining step, for example (see 8, lines 20-67). Therefore, **claims 9, 17, 28, and 41** are rejected on the same rationale as the rejection of **claims 5, 19, 27, and 37**.

5. **Claims 6-8, 20-22, 30-32, and 38-40** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2001/0037458 to **Kean** in view of US Patent 6,587,978 to **Merritt et al.**.

5.1 **As per claims 6-8, 20-22, 30-32, and 38-40, Kean** substantially teaches the claimed method and apparatus of claims 1, 12, 23, and 33. **Kean** also discloses generating fingerprint from a plurality of circuit elements, for example (see page 10, paragraphs 0134-0141). **Kean** also suggests create wires which attach to the key input in complicated pattern into the surrounding circuit and changing conductive layer and direction at regular intervals to make it difficult for an attacker to trace them. **Kean** does not explicitly disclose counting the number of oscillations although such technique is well known in the art to generate fingerprint. However, **Merritt et al.** in an analogous art teaches counting the number of oscillations of an oscillator on the FPGA during a predetermined time interval, for example (see column 4, lines 22-50), wherein the oscillator comprises configurable logic block, counting the number of oscillations of a first oscillator on the FPGA during a predetermined time interval, for example (see column 4, lines 22-67); counting the number of oscillations of a second oscillator on the FPGA during the predetermined time interval, for example (see column 4, line 22 through

column 5, line 16); and generating a ratio between the resultant first and second oscillator counts that is used as the fingerprint, for example (see column 4, line 22 through column 5, line 16). **Merritt et al.** also discloses that controlling pulse width and periods of internal control signals also reduces costs and saves valuable manufacturing time, for example (see column 6, lines 42-60). Therefore, it would have been obvious to one of ordinary skill in the art of integrated circuit at the time the invention was made to modify the method of **Kean** to measure propagation delays for a plurality of circuit elements on the FPGA and combine the propagation delays to generate the fingerprint as taught by **Merritt et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Merritt et al.** so as to an electronic test key that varies pulse widths and/or periods, and frequencies of other control signals (column 7, lines 7-20) to stress, for instance, the memory device, it prevents failure on a simple test and it provides good production feedback as to where the lockout delays should be adjusted (column 6, lines 4-67) this implementation will eventually reduce costs and save valuable manufacturing time.

6. **Claims 10, 11, 18, 29, and 42-43** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2001/0037458 to **Kean** in view of US Patent 6,185,126 to **Rodgers et al.**.

6.1 **As per claims 10, 11, 18, 29, and 42-43, Kean** substantially teaches the claimed method and apparatus of claims 1, 12, 23, and 33. **Kean** also discloses generating fingerprint from a plurality of circuit elements, for example (see page 10, paragraphs 0134-0141). **Kean** also

suggests encoding keys by creating wires which attach to the key input in complicated pattern into the surrounding circuit and changing conductive layer and direction at regular intervals to make it difficult for an attacker to trace them, and further discloses using voltage variations to generate fingerprint, (for example (see page 10, paragraphs 0134-0135). **Kean** does not explicitly disclose the steps in using transistor pairs. However, **Rodgers et al.** in an analogous art teaches using differences in transistor threshold voltages caused by manufacturing process variations to generate the fingerprint, for example (see column 2, lines 13-30 and column 3, lines 1-30) and the limitation of wherein generating the fingerprint further comprises: applying a read voltage to a plurality transistor pairs; determining, for each transistor pair, whether a first transistor or a second transistor of the pair turns on earlier; generating, for each transistor pair, a corresponding bit of the fingerprint in response to the determining step, for example (see column 5, line 35 through column 6, line 12). **Rodgers et al** discloses a method that makes an interconnection or logic cells predictable, for example implementing embedded macrofunctions and allows the logic so implemented to be available immediately upon power-up (column 8, lines 28-36). **Rodgers et al.** also discloses that this method has the advantage of eliminating the need for a separate programming operation following power-up, for example (see column 5, line 35 through column 6, line 12). Therefore, it would have been obvious to one of ordinary skill in the art of integrated circuit at the time the invention was made to modify the method of **Kean** by implementing the method of **Rodgers et al**: generating, for each transistor pair, a corresponding bit of the fingerprint in response to the determining step as to encode the key signal as taught by **Rodgers et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Rodgers et al.** so as to encode the key

signal by implementing embedded macrofunctions and allowing the logic so implemented to be available immediately upon power-up thus eliminate the need for a separate programming operation following power-up.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7.1 a) The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses methods of generating keys from voltage threshold, number of oscillations etc..

US Patents: 5,961,577 Soenen et al ; 5,450,360 Sato; 6,150,837 Beal et al. 5,007,087 Bernstein et al ; 4,203,070 Bowles et al ; 5,952,933 Issa et al ;

b) US Patent: 5,970,142 to Erickson, also discloses many of the claimed features such as generating fingerprint, transmitting encrypted data, etc.

7.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin
Patent Examiner
February 1, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100